Solicitation FCIS-JB-980001-B
FSC Group 70
SIN 132-62

Homeland Security Presidential Directive (HSPD-12) Product and Service Components

Personal Identity Verification (PIV) Card Management and Production Services and Products

Statement of Qualification Requirements

Date: June 19, 2006
Revised: August 30, 2006

GSA
U.S. General Services Administration
Federal Acquisition Service

Change Control Page

Date	Description
6/19/2006	Initial release of the PIV Qualification Requirements
8/30/2006	Revised Appendix A to require submission of completed compliance matrix.

TABLE OF CONTENTS

List of Tables

List of Figures

1.0 Overview

General Services Administration (GSA) Federal Acquisition Service (FAS) requires the Contractor to provide the supplies and services necessary to support a common, interoperable, multi-application HSPD-12 PIV card solution as specified in this document. The HSPD-12 PIV program allows Federal agencies, activities, and organizations to select from multiple and flexible solutions to meet HSPD-12 PIV requirements. The Contractor will be called upon to provide HSPD-12 PIV compliant services and products under individual task/delivery orders issued in accordance with FSC Group 70 Special Item Numbers (SIN):

- 132-60, Access Certificates for Electronic Services (ACES) Program (SIN 132-60).
- 132-61, PKI Shared Service Providers (PKI SSP) Program (SIN 132-61).
- 132-62, HSPD-12 Product and Service Components (SIN 132-62).

This Statement of Qualification Requirements establishes the qualification requirements for providing PIV card management and production services and products under SIN 132-62.

1.1 Background

Authentication services and products provide for authentication of individuals for purposes of physical and logical access control, electronic signature, and performance of E-business transactions and delivery of Government services. Authentication Services and products consist of hardware, software components and supporting services that provide for identity assurance.

HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Further, the Directive requires the Department of Commerce to promulgate a Federal standard for secure and reliable forms of identification within six months of the date of the Directive. As a result, the National Institute of Standards and Technology (NIST) released Federal Information Processing Standard 201: Personal Identity Verification of Federal Employees and Contractors (FIPS 201) on February 25, 2005. FIPS 201 requires that the digital certificates incorporated into the PIV identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. In addition, FIPS 201 requires that Federal identity badges, referred to as PIV credentials, issued to Federal employees and contractors comply with the Standard and associated NIST Special Publications 800-73, 800-76, 800-78, and 800-79.

HSPD-12 requires that the Federal credential (the PIV card) be secure and reliable, which is defined as a credential that:

- Is issued based on sound criteria for verifying an individual's identity.
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- Can be rapidly authenticated electronically.
- Is issued only by providers whose reliability has been established by an official accreditation process.

In support of this goal, GSA's Office of Governmentwide Policy (OGP) and FAS share responsibility for the design, development, implementation, operation, and maintenance of the HSPD-12 PIV Program.

This Statement of Qualification Requirements, under SIN 132-62, provides the specification of minimum technical functions and capabilities related to the HSPD-12 PIV card management and production services and products. Contractors must meet the qualification requirements as specified in order to be considered for contract award under SIN 132-62 for HSPD-12 PIV card management and production services and products, which provide for authentication of individuals for purposes of physical and logical access controls, electronic signature, performance of e-business transactions, and delivery of government services.

At a minimum, the ordering organization can use an HSPD-12 PIV card as a Federal employee or agency Contractor requiring physical and logical access to Federal facilities and networks. The Contract under SIN 132-62 offers a vehicle to issue PIV cards that can be used to provide basic visual identification, electronic identification and authentication for physical and logical access control, cryptographic services, biometrics functions, as well as a number of value added features. The PIV card contains information carried on a processing chip that could be used commonly across applications.

1.2 Objectives

The objectives of the HSPD-12 PIV services and products are to:

(1) Achieve best value for PIV cards and services by aggregating Government requirements.

(2) Provide government agencies and other ordering activities with robust PIV services.

(3) Achieve maximum efficiency by procuring PIV services from existing commercially available products, systems, and services, to the extent possible.

(4) Achieve maximum efficiency in procuring PIV services by encouraging partnership arrangements among commercial entities.

(5) Achieve implementation of a trust model which features

(6) Use of a single PIV card and PIV digital credentials for physical and logical access to Government facilities and information systems.

(7) Quality assurance and inspection of Contractor's practices for adherence to terms of HSPD-12 and FIPS 201.

(8) Achieve intra-operability among the functional components within an enterprise PIV services solution and interoperability across Government implementations by defining a set of standard methods for issuing and accessing standard PIV card data in accordance with FIPS 201 and related technical specifications [1].

[1] All references to FIPS 201 throughout this document incorporate references to the latest release versions of FIPS 201 and all related NIST Special Publications and technical specifications.

2.0 PIV Card System Description

The PIV card system, as described, will provide the security, privacy, and interoperability as required in HSPD-12 and FIPS 201. The HSPD-12 implementation components specified under SIN 132-62 are as follows:

- PIV enrollment and registration services and products.
- PIV systems infrastructure services and products.
- PIV card management and production services and products.
- PIV card activation and finalization services and products.
- Physical access control services and products.
- Logical access control services and products.
- PIV system integration services and products.
- Approved FIPS 201-compliant services and products.
- Professional services to support implementation and integration for ordering activities and applications.

The PIV categories of systems, products, and services are those that are required to manage users and their cards through the entire PIV card life cycle. Associated systems include those that interact with the system and either provide information or use information from the system, such as the Office of Personnel Management (OPM) in checking the suitability of applicant information provided by the registration/enrollment system and agency Identity Management Systems (IDMS) that provide access control and other identity information specific to agency requirements.

Summary definitions of the categories of PIV systems, products, and services are provided in the following sections.

2.1 Enrollment and Registration Services and Products

The enrollment and registration services and products relate to the process of collecting identity information from a PIV applicant and distributing that information to other component systems and services within the PIV system, such as the PIV systems infrastructure. The applicant will be "sponsored" by a government employee. Enrollment and registration functions will be provided via processes that enable the enrollment and registration to be "local" to the applicant.

2.2 PIV Systems Infrastructure Services and Products

The PIV systems infrastructure services and products relate to provision of a set of business process functions that manages the PIV workflow among and between other PIV system components. Specifically, PIV systems infrastructure services and products provide the software functionality required to manage PIV credentials, including IDMS and Card Management Systems (CMS).

2.3 PIV Card Management and Production Services and Products

The PIV card management and production services and products relate to card lifecycle management, including card production, personalization, printing, internal configuration for use, and delivery of the card for finalization and issuance.

2.4 PIV Card Activation and Finalization Services and Products

The PIV card activation and finalization services relate to final issuance of the PIV card to the applicant including verification of identity of the applicant, verification of PIV card operation, final configuration of Public Key Infrastructure (PKI) components, and obtaining signatures from the applicant verifying receipt of the card.

2.5 Physical Access Control Services and Products

The physical access control services and products and products relate to the provision of the functions required to provide card holders with access to government controlled facilities. The physical access control services and products interface directly and indirectly with other PIV system components and agency-specific systems.

2.6 Logical Access Control Services and Products

The logical access control services and products relate to provision of the functions required to provide card holders with access to government controlled IT networks and computer systems. The logical access control services and products interface directly and indirectly with other PIV system components and agency-specific systems.

2.7 PIV System Integration Services and Products

The PIV system integration services products relate to provision of integrated PIV system components, products, and services. It also relates to integration of PIV system components with existing agency systems and infrastructures.

2.8 Approved FIPS 201-Compliant Services and Products

Approved FIPS 201-compliant services and products relate to provision of services and products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. NIST has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform card and reader interface testing for interoperability.

2.9 Professional Services

Professional services relates to provision of support for implementation and integration for ordering activities and applications.

2.10 PIV Associated Systems

2.10.1 Agency-Specific IIDMS

Agency-specific IDMS will maintain access control and other identity information as may be required by the agency to manage physical and logical access to the agency.

2.10.2 OPM/Federal Bureau of Investigation (FBI)

All PIV applicant background investigations will be conducted through the OPM. OPM will conduct the investigations and forward results to the appropriate agency and/or PIV system component. The FBI will be responsible for conducting fingerprint checks against its fingerprint databases as a component of all background investigations and will interface directly and indirectly with OPM and the appropriate PIV system component.

2.11 PIV Roles

The following roles are used throughout this Statement of Qualification Requirements to describe individuals who perform PIV functions:

(1) **Applicant -** The individual to whom a PIV credential needs to be issued.

(2) **PIV Sponsor -** The individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.

(3) **Enrollment Official -** The entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The

PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant.

(4) **Issuer -** The entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

(5) **PIV Digital Signatory -** The entity that digitally signs the PIV biometrics and CHUID.

(6) **PIV Authentication Certification Authority (CA) -** The CA that signs and issues the PIV Authentication Certificate.

The principle of separation of duties will be enforced to ensure that no single individual has the capability to issue a PIV card without the participation of another authorized person. The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

The applicant appears in-person at least once before the issuance of a PIV card.

2.12 Conceptual Overview of PIV Components

Figure 2.12-1, Conceptual Overview of PIV components, provides a high-level overview of the PIV components and functionalities. At the time of implementation and based on agency requirements, the order of the functions and processes may differ from the numbered order illustrated.

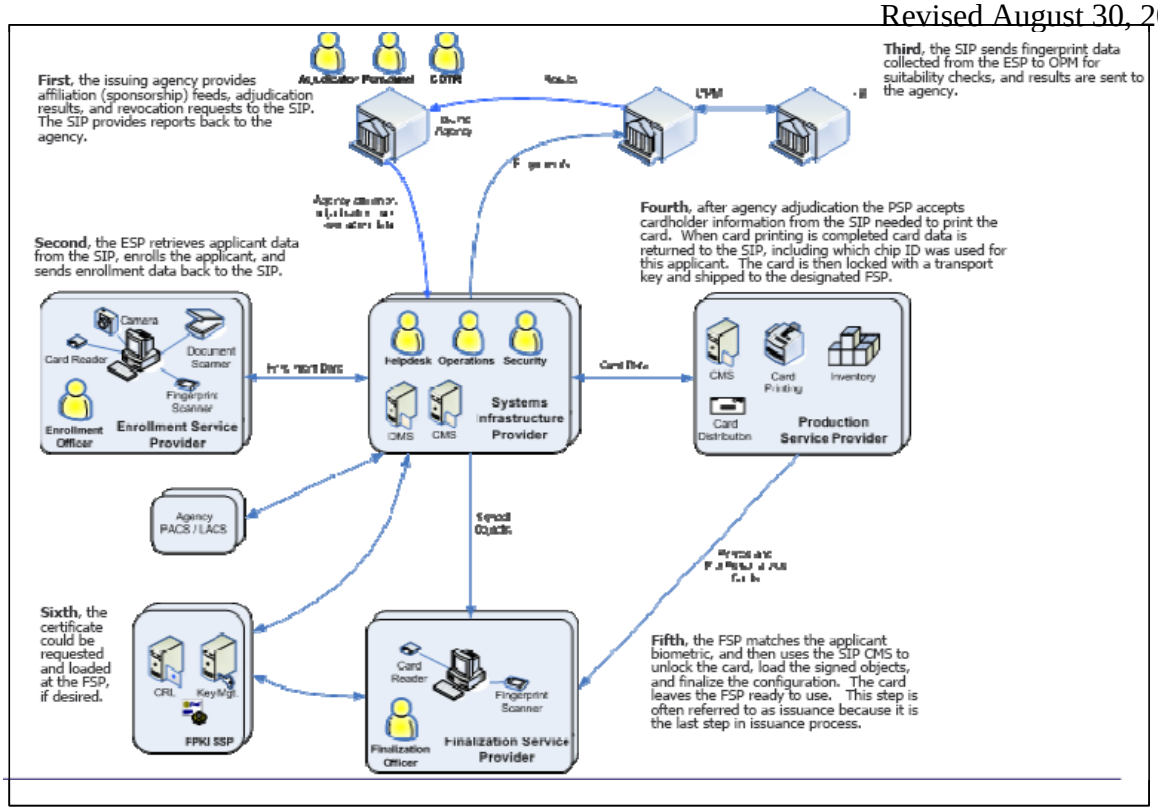

Figure 2.12-1. Conceptual Overview of PIV Components

2.13 PIV Card Management and Production Components

Figure 2.13-1, PIV Card Management and Production Components, depicts the components that incorporate the scope of the qualifications document.

Figure 2.13-1. PIV Card Management and Production Components

3.0 PIV Card Management and Production Services and Products Qualification Requirements

This Statement of Qualification Requirements under SIN 132-62 provides the specification of minimum technical functions and capabilities related to the provision of HSPD-12 PIV card management and production services and products. Contractors must meet the qualification requirements as specified in order to be considered for contract award under SIN 132-62 for HSPD-12 PIV card management and production services and products.

The Contractor shall have the capability to provide card management and production of PIV applicants. The Contractor shall have the capability to store, and maintain all information and documentation related to production of an applicant's card. Identity information and various types of biometric data (e.g., fingerprints, photographs) shall be stored, transmitted, and processed IAW FIPS 201.

The Contractor shall have the technical capability to provide one or more services and products in the following categories:

(1) Card management and production hardware and software products.

(2) Card deployment services.

(3) Managed card management and production services.

The Contractor shall have the capability to provide HSPD-12 PIV compliant and GSA approved services and products.

Contractors shall have the capability to provide individual hardware and software products and/or complete standard configuration card management and production stations.

All services and products related to the PIV card for which compliance is required must comply with HSPD-12, FIPS 201, applicable NIST Special Publications and/or GSA interoperability compliance requirements. For categories of services and products that require GSA approval (see http://fips201ep.cio.gov/index.php), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant services and products relate to provision of services and products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. NIST has established the NIST NPIVP to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other products needed for agency implementation of

HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform card and reader interface testing for interoperability.

3.1 Scope and Description of Qualification Requirements

The scope and descriptions of the qualification requirements for provision of HSPD-12 PIV card management and production services and products are defined in the following sections. Table 3.1-1, List of Card Management and Production Services and Products Qualification Requirements, provides a list of the qualification requirements the Contractor shall address and indicates the applicable section reference for each item.

Table 3.1-1. List of Card Management and Production Services and Products Qualification Requirements

Requirement No.	Description	Section References
Card Management and Production Hardware and Software Products		
1.	Card Management and Production Hardware and Software Products	3.1.1.
2.	Technical Standards Compliance	3.1.1.1
3.	Interface and Interoperability Support	3.1.1.2
4.	Card Management and Production Software	3.1.1.3
5.	Security Standards Compliance	3.1.1.4
6.	Hardware and Software Maintenance Support	3.1.1.5
7.	Special Contract Requirements	3.1.1.6
8.	Allowance for Technology Changes	3.1.1.7
9.	Contractor Personnel Training	3.1.1.8
10.	Administrative and Personnel Security	3.1.1.9
11.	Deliverables	3.1.1.10
12.	Response Package Submission	3.1.1.11
Card Management and Production Deployment Services		
13.	Card Management and Production Hardware and Software Compliance	3.1.2.
14.	Training	3.1.2.2

Requirement No.	Description	Section References
15.	Customer Service Center	3.1.2.3
16.	Special Contract Requirements	3.1.2.4
17.	Availability of Services	3.1.2.5
18.	Response Time for Services	3.1.2.6
19.	Scalability and Implementation Schedule	3.1.2.7
20.	Allowance for Technology Changes	3.1.2.8
21.	Past Performance	3.1.2.9
22.	Contractor Personnel Training	3.1.2.10
23.	Administrative and Personnel Security	3.1.2.11
24.	Deliverables	3.1.2.12
25.	Project Management Office	3.1.2.13
26.	Response Package Submission	3.1.2.14
Managed Card Management and Production Services		
27.	Card Management and Production Hardware and Software Compliance	3.1.3.1
28.	Card Management and Production Deployment Services Compliance	3.1.3.2
29.	Audit, Logging, and Standard Reporting	3.1.3.3
30.	Technical Standards Compliance	3.1.3.4
31.	Interface and Interoperability Support	3.1.3.5
32.	Security Certification and Accreditation (C&A) and Re-Accreditation	3.1.3.6
33.	Date/Time Stamp Synchronization	3.1.3.7
34.	Performance	3.1.3.8
35.	Customer Service Center	3.1.3.9
36.	Privacy Act Requirements	3.1.3.10
37.	Contractor Personnel Training	3.1.3.11

Requirement No.	Description	Section References
38.	Data Transfer	3.1.3.12
39.	Security/Privacy Requirements	3.1.3.13
40.	Past Performance	3.1.3.14
41.	Deliverables	3.1.3.15
42.	Project Management Office	3.1.3.16
43.	Response Package Submission	3.1.3.17
Pricing		
44.	Pricing	3.2

3.1.1 Card Management and Production Hardware and Software Products

The Contractor shall have the capability to provide card management and production hardware and/or software products to be purchased and owned by an ordering entity (i.e., agency) that includes the following functional requirements to capture, store, and process PIV cards and maintain card management and production information:

(1) PIV cards: The Contractor shall have the capability to provide FIPS 201 PIV compliant cards, as follows:

(a) The Contractor shall have the capability to obtain and maintain a sufficient inventory of PIV compliant raw card stock and supplies (i.e., laminate ribbon, thermal ink) in a secure environment to support ordering entities.

(b) The Contractor shall have the capability to receive raw card stock from the manufacturer who will securely ship and track each card for receipt at the card production facility.

(c) The Contractor shall have the capability to maintain full inventory control of blank initialized or pre-issued (e.g. with the manufacturers keys) stock, consumables and manufacturing materials;

(d) The Contractor shall have the capability to periodically verify correctness and quality of fixed (non-Applicant) internal configurations.

(e) The Contractor have the capability to deliver quantities of cards via secure shipping and delivery processes, including delivery tracking and confirmation, only to authorized locations and authorities.

(2) CMS: The Contractor shall have the capability to provide a CMS, including all hardware and software, that shall, at a minimum, provide the following functionalities:

(a) Implementation of interfaces with other authorized PIV systems infrastructure components (i.e., IDMS) and PKI CAs to receive and send applicant data to for the purposes of card personalization, card updates, and configuration of PKI certificates.

(b) Completion of electronic personalization of PIV card IAW FIPS 201, Section 4.1, Physical Card Topology, including all mandatory and optional data, and NIST and GSA FIPS 201 Evaluation Program specifications, including the following:

(1) Personalization of the physical (visual surface), including printing photographs, names, and other information

(2) Personalization of the logical (contents of the ICC), as follows:

(a) Loading of card applications and biometrics
(b) Performing card management key generation
(c) Creating unique identifier (CHUID)
(d) Performing key generation for digital certificates
(e) Obtaining and loading digital certificates.

(c) Activation of the card for card updates via challenge response protocol using cryptographic keys stored on the card that are specific to each card.

(d) Key management for the generation of key pairs, issuance and distribution of digital certificates throughout the card life cycle.

(e) Maintenance of card production lifecycle information, from receipt of request to produce the PIV card to delivery of the configured and personalized PIV card to the issuer's location.

(f) Support for secure backup of all data related to card holder and card history information.

(g) Full operation and on-line availability 24 hours per day and seven (7) days per week to accept card production requests, status updates, and for on-line functions in support of other authorized PIV system services and other normal business functions.

(h) Sufficient database capacity.

(i) Access controls that permit only authorized and authenticated users and system transactions.

(j) Storage and maintenance of the following card data:

(1) Mandatory card data:
- (a) Photograph
- (b) Name
- (c) Employee Affiliation
- (d) Organizational Affiliation
- (e) Expiration Date
- (f) Agency Card Serial Number
- (g) Issuer Identification
- (h) PIN
- (i) Cardholder Unique Identifier (CHUID)
- (j) PIV authentication certificate
- (k) Biometric fingerprints
- (l) PIV authentication certificate

(2) Optional card data:
- (a) Cardholder signature
- (b) Agency specific text
- (c) Rank
- (d) Portable Data File (PDF) Two-Dimensional Bar Code Information
- (e) Header
- (f) Agency Seal
- (g) Footer
- (h) Issue Date
- (i) Color-Coding for Employee Affiliation
- (j) Photo Border for Employee Affiliation
- (k) Agency-Specific Data
- (l) Return to Information
- (m) Physical Characteristics of Cardholder
- (n) Additional Language for Emergency Responder Officials
- (o) Standard Section 499, Title 18 Language
- (p) Linear 3 of 9 Bar Code information
- (q) Agency-Specific Text
- (r) Certificate for Digital Signatures
- (s) Certificate for Key Management
- (t) Asymmetric or Symmetric Card Authentication Keys for Supporting PACS
- (u) Symmetric Key(s) associated with the CMS

(g) Data maintenance, retention, and disposition capabilities IAW with the Federal laws, standards, regulations, and guidelines, including the Privacy Act of 1974.

(h) Maintenance of the list of approved systems PIV system components (i.e., IDMS, Issuers) that can submit PIV requests for card product.

(i) Acknowledgment of request to produce a PIV card.

(j) Notification to approved system infrastructure components upon completion of PIV card production.

(k) Secure transmission and receipt of applicant data to provide for integrity and confidentiality of the data only from authorized PIV systems.

(3) Card Printer Stations: The Contractor shall have the capability to provide PIV card printer stations standard hardware and software configurations as follows:

(a) Printer workstation that meets all of the GSA FIPS 201 Evaluation Program specifications for card printer stations, including peripherals, with enough ports to connect all of them simultaneously.

(b) Printer workstation with standard configuration (i.e., operating system, hardware, and software) to provide all of the NIST and GSA FIPS 201 card printer station functions.

(c) Capability to control access only to authorized operators and system administrators based on PIV card authentication.

(d) Capability to receive card personalization information via secure, authenticated transmission to provide integrity and confidentiality of the data.

(e) Capability to send card personalization successful and unsuccessful completion notifications to other PIV system components.

(f) Secure delivery of required quantities in accordance with order entity requirements in accordance with secure shipping and delivery processes, including delivery tracking and confirmation, only to authorized locations.

(g) Inventory control system.

(h) Audit and logging of card printer station transactions including individual accountability for applicable functions completed.

(4) Ancillary Parts: Ancillary parts and/or hardware shall, at a minimum, provide the following:

(a) Optical mouse.

(b) Power cords and all connector cables.

(c) Surge protectors.

(d) Accessory lights.

(5) Shipping cases: Shipping cases, shall a minimum, provide the following:

(a) Hardware components shall fit into a maximum of two ruggedized suitcases with pre-shaped foam packaging, each weighing no more than 35 pounds. Suitcases shall be lightweight, durable and theft deterrent (locks, cables, tracking barcodes, etc.).

3.1.1.1 Technical Standards Compliance

All card management and production products related to the PIV card for which compliance is required must comply with HSPD-12, Federal Information Processing Standard 201 (FIPS 201), applicable National Institute of Standards and Technology (NIST) Special Publications (SP) and/or GSA interoperability compliance requirements. For categories of card management and production products that require GSA approval (see http://fips201ep.cio.gov/index.php), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant products relate to provision of products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. NIST has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform tests for interoperability.

The Contractor shall have the capability to provide documentary evidence of FIPS 201 and GSA interoperability approval, or a plan to ensure that all products are fully compliant, for those hardware and software products that require FIPS 201 and GSA interoperability compliance

3.1.1.2 Interface and Interoperability Support

To support communications with authorized officials and users, the hardware and software shall,

at a minimum, support World Wide Web (WWW) Internet network access and interfaces for telecommunications services. The products shall support other network access interfaces and/or protocols as agreed between the ordering activity and the Contractor.

The products shall have the capability to implement software and interfaces that provide digital signature, authentication, data integrity, and privacy of personal data at rest and during transmission.

The PIV interface specification to support interoperability between PIV components provided by other Contractors and/or ordering entities (i.e., agencies) is currently under development. The Contractor shall have the capability to implement and support the PIV interface specification, at the time the PIV interface specification is published and required for all Contractors under SIN 132-62.

3.1.1.3 Card Management and Production Software

The Contractor shall have the capability to provide card management and production software that, at a minimum, provides the following:

(1) ”Programmable screens” for card management and production data input and output to support all CMS and card printer station functionalities.

(2) Section 508-compliant software interfaces for use by agency operators and end-users.

(3) Output of the data in compliance with the data model and PIV object identifier requirements specified in FIPS 201 and NIST SP 800-76.

3.1.1.4 Security Standards Compliance

The Contractor shall have the capability to comply with FIPS 201, Appendix B, PIV Validation, Certification, and Accreditation, requirements.

3.1.1.5 Hardware and Software Maintenance Support

The Contractor shall, at a minimum, have the capability to provide support for hardware replacements in the event of hardware component failure, updates, and/or maintenance as follows:

(1) If there is a component failure, the Contractor shall have the capability to ship replacements via next day shipping to minimize station down-time.

(2) The Contractor shall have sufficient spare equipment on hand.

The Contractor shall have the capability to provide for update and maintenance of the associated product software as required to support modifications, enhancements, and license maintenance fees.

3.1.1.6 Special Contract Requirements

The Contractor shall have the capability to comply with the special contract requirements specified in SIN 132-62.

3.1.1.7 Allowance for Technology Changes

The Contractor shall create and have the capability to provide a robust infrastructure with sufficient flexibility to incorporate appropriate evolving technology.

The Contractor shall be able to incorporate new algorithms, formats, technologies, mechanisms, and media after contract award, as appropriate and approved by Government. The Government recognizes that technologies are rapidly evolving and advancing. The Government wishes PIV card services, features, etc. to remain up-to-date with commercial equivalents. Accordingly, the Government anticipates that services, features, etc., available under SIN 132-62 will be increased, enhanced, and upgraded as these improvements become available.

The Contractor shall provide the capability to continue compliance and re-approval with NIST and GSA requirements for those services and products that require approval, throughout system and product lifecycle and technology changes.

Contractor shall propose enhancements which reduce the Government's risk, meet new or changed Government needs, improve performance, or otherwise present a service advantage to the Government.

3.1.1.8 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV services, HSPD-12, and FIPS 201. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.1.9 Administrative and Personnel Security

The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing system configuration (i.e., operating system, software, and peripheral installations and configuration) for standard configuration stations.

3.1.1.10 Deliverables

The Contractor shall have the capability to provide the deliverables as specified in Table, 3.1.1.10-1, Deliverables.

Table 3.1.1.10-1. Deliverables

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
1	Card management and production approved hardware and software products.	As required in requests.	As required in request.	As required in request.	As required in request.
2	Standard configuration PIV cards, CMS, and printer stations.	As required in requests.	As required in request.	As required in request.	As required in request.
3	A record of the transaction audit data resulting from deployment of the hardware and software products.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.
4	Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
5	Program management reports providing information used to manage the PIV services.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
6	System fraud and security reports that will assist in the detection of fraud and ensure system security.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
7	Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or a plan to obtain approval.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
8	Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media)	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
9	Provide assurance of the trustworthiness and competence of employees.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
10	Fraud protection procedures	As required in request	As required in request	As required in request	60 calendar days from contract award
11	Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse	As required in request	Electronically, mail, or facsimile	As required in request	Immediatel y
12	Technical meetings	As required in request	As required in request	As required in request	As required in request
13	Monthly reports	One (1)	Electronic access, plus 1 paper copy	As required in request	Within 10 business days of the end of the month covered in the report.

3.1.1.11 Hardware and Software Products Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the card management and production hardware and software products qualification requirements specified in this document as follows:

(1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified.

(2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services), the Contractor may provide a consolidated response.

(3) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA approval for those products that require FIPS 201 and GSA approval, as specified in Section 3.1.1.1.

(4) Documentary evidence of competence of employees as specified in Section 3.1.1.8 of this document.

(5) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.1.9 of this document.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.1.2 Card Management and Production Deployment Services

The Contractor shall have the capability to provide PIV card deployment services to agency locations, whether the Contractor or the agency owns, operates, and manages the card management and production hardware and software.

The Contractor shall have the capability to provide the following PIV card management and production support functionalities:

(1) Centralized configuration to complete initial configurations of card management and production hardware and software.

(2) Capability to apply software changes in a centralized model, including testing and minimal on-site steps.

(3) Comprehensive inventory control including provision of on-line access to authorized authorities and PIV system components.

(4) Secure shipping, including tracking capabilities only to authorized locations and authorities.

(5) Setup instructions for installation at government sites.

(6) On-site installation support.

(7) Card management and production personnel services as may be required.

3.1.2.1 Card Management and Production Hardware and Software Compliance

The Contractor shall have the capability to provide card management and production hardware and software products as part of deployment services that comply with all requirements specified in Section 3.1.1 of this document as part of deployment services.

3.1.2.2 Training

The Contractor shall have the capability to provide card management and production training to government personnel specifically as follows:

(1) In-person training. The Contractor shall have the capability to provide in-person training for government personnel who are performing card management and production functions. The Contractor shall have the capability to provide in-person training at government locations and at Contractor provided training facilities.

(2) On-line training: The Contractor shall have the capability to provide computer based training for agency personnel who are performing card management and production services with the following functionalities:

(a) Capability to provide complete information on the card management and production process.

(b) Capability to be available and tracked via one of the approved government on-line training sites.

(c) Capability to test the trainee's competence and understanding of the information.

(3) On-line installation video: The Contractor shall have the capability to provide an on-line installation video that is made available via the Internet and on the desktop to provide on-site installation processes and typical troubleshooting steps, including a "quick-help guide" for agency personnel performing on-site installation and configuration of card management and production hardware and software.

3.1.2.3 Customer Service Center

The Contractor shall have the capability to provide a customer service center to provide help desk and other support functionalities for agency card management and production personnel as follows:

(1) The capability to provide the following services for ordering agencies:

(a) Services, features, and options.

(b) Troubleshooting and problem reporting.

(c) Billing questions and issues.

(d) Implementation of services.

(2) The capability to provide a toll free number and on-line access for problem reporting and troubleshooting.

(3) The capability to provide customer service center usage and activity data.

(4) The capability to be available 24 hours a day, 7 days per week.

(5) The capability to provide voice mail to handle incoming calls received at times when assigned staff is unavailable.

(6) The capability to provide on-line information and support (e.g., maintenance of a web site for posting Frequently Asked Questions (FAQs) and general information).

(7) The capability to provide an e-mail address for communicating with the customer service center.

(8) The capability to respond to e-mail messages received automatically with a prompt acknowledgement of receipt and respond to content within 30 minutes.

(9) The capability to implement and maintain a system for receiving, recording, responding to, and reporting customer service problems within its own organization and to the government.

(10) The capability to implement and maintain a system of records relating to customer requests for services and the services provided. For each such request, the Contractor shall record sufficient information in order for the Government to determine who requested assistance, when the request was submitted, what action was required and/or resolution of the issue, and when the issue was resolved. At a minimum, the Contractor shall record the following information for each customer service request:

(a) Date/time initially contacted.

(b) Method of contact (e.g., telephone, e-mail, etc.).

(c) Name of individual making the contact.

(d) Type of service requested or problem reported.

(e) Action taken.

(f) Date/time action completed.

(g) Name of person taking the action.

(h) Requirements for follow-up action (if any).

(i) Date/time report filed.

(j) Name of person filing report.

(k) Capability for customer service records to be made available for

Government review or quality assurance inspection upon request.

3.1.2.4 Special Contract Requirements

The Contractor shall have the capability to comply with the special contract requirements specified in SIN 132-62.

3.1.2.5 Availability of Services

All of the on-line services and products specified shall, at a minimum, be in operation and available for use during the required hours of operation, not less than 99.5 percent of the time calculated on a monthly basis.

3.1.2.6 Response Time for Services

The Contractor shall, at a minimum, have the capability to provide the specified services according to the response times set forth in Table 3.1.2.6-1. All response times shall be measured from the time the Contractor receives an initiation message in its inbound queue until the time the Contractor's response leaves its outbound queue (i.e., from the time a request message is received until the time the response message is transmitted to the requestor).

Table 3.1.2.6-1. Response Time Requirements

Transaction/Process	Response Time	Constraints
On-site technical assistance	5 days	>= 95% of all transactions within response
Response to trouble call	30 minutes	>= 95% of all transactions within response
Replacement of hardware/software due to component failures	Next day shipping	>= 95% of all transactions within response

3.1.2.7 Scalability and Implementation Schedule

The Contractor shall have the capability to provide a robust infrastructure to provide scalability and performance to support the service requirements of the ordering activity applications and IAW with the requirements in this Statement of Qualification Requirements.

The Contractor shall have the capability to provide an implementation schedule and plan that provides the required functionalities.

3.1.2.8 Allowance for Technology Changes

The Contractor shall create and have the capability to provide a robust infrastructure with sufficient flexibility to incorporate appropriate evolving technology.

The Contractor shall be able to incorporate new algorithms, formats, technologies, mechanisms, and media after contract award, as appropriate and approved by Government. The Government recognizes that technologies are rapidly evolving and advancing. The Government wishes PIV card services, features, etc. to remain up-to-date with commercial equivalents. Accordingly, the Government anticipates that services, features, etc., available under SIN 132-62 will be increased, enhanced, and upgraded as these improvements become available.

Contractor shall propose enhancements which reduce the Government's risk, meet new or changed Government needs, improve performance, or otherwise present a service advantage to the Government.

3.1.2.9 Past Performance

The Contractor shall have the capability to provide detailed descriptions of past performance and prior experience related to large-scale government and/or non-government similar implementations for the Contractor and any member of the Contractor's team (e.g., subcontractor, joint venture, etc.) responsible for providing an estimated 25% or more of the services and products provided under an awarded contract.

The Contractor shall have the capability to provide information related to past performance and prior experience for the Contractor's largest projects (considering dollar value) completed or ongoing with an end date for each selected project not more than two years prior to the release of this Statement of Qualification Requirements.

The Contractor shall have the capability to provide the following past performance and prior experience information related to the Contractor's selected projects:

(1) Compliance with technical or functional specifications or requirements.

(2) Technology refreshment.

(3) Quality of services and products;

(4) Adherence to schedules.

3.1.2.10 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV services, HSPD-12, and FIPS 201. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.2.11 Administrative and Personnel Security

The Contractor shall have the capability to ensure the integrity of deployment service operations including all personnel involved in system administration, security administration, card management and production operators, on-site installation, troubleshooting, and training, and system configuration (i.e., operating system, software, and peripheral installations and configuration), services. The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing managed service operations.

3.1.2.12 Deliverables

The Contractor shall have the capability to provide the deliverables as specified in Table, 3.1.2.12-1, Deliverables.

Table 3.1.2.12-1. Deliverables

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
1	Deployment services as specified.	As required in requests.	As required in request.	As required in request.	As required in request.
2	A record of the transaction audit data resulting from provision of deployment services.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.
3	Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
4	Program management reports providing information used to manage the PIV services.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
5	System performance reports that monitor the operation and performance of the PIV services.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
6	System fraud and security reports that will assist in the detection of fraud and ensure system security.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
7	Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or a plan to obtain approval.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
8	Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media)	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.

No.	Descriptions of Deliverable	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
9	Provide assurance of the trustworthiness and competence of employees.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
10	Fraud protection procedures	As required in request	As required in request	As required in request	60 calendar days from contract award
11	Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse	As required in request	Electronically, mail, or facsimile	As required in request	Immediately
12	Trouble reports status	As required in request for procedures	Electronically, mail, or facsimile	As required in request	Within 4 hours after first report, updated every 4 hours thereafter
13	Technical meetings	As required in request	As required in request	As required in request	As required in request
14	Monthly reports	One (1)	Electronic access, plus 1 paper copy	As required in request	Within 10 business days of the end of the month covered in the report.
15	Information related to past performance as specified.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
16	Implementation schedule and plan.	As required in request.	As required in request.	As required in request.	As required in request.

3.1.2.13 Project Management Office

The Contractor shall have the capability to provide a Project Management Office (PMO) to oversee all facets of the deployment services, including tracking of all PIV card management and production hard and software deployment status and locations.

3.1.2.14 Card Management and Production Deployment Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the card management and production deployment services qualification requirements specified in this document as follows:

(1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified, specifically the following "core" requirements:
   i. All technical and functional requirements.
   ii. Past performance and experience in implementation of similar and/or equivalent enterprise services.

(2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services), the Contractor may provide a consolidated response.

(3) Documentary evidence of past performance as specified in Section 3.1.2.9 of this document.

(4) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA approval for those products that require FIPS 201 and GSA approval as specified in Section 3.1.1.1.

(5) Documentary evidence of competence of employees as specified in Section 3.1.2.10 of this document.

(6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.2.11 of this document.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.1.3 Managed Card Management and Production Services

The Contractor shall have the capability to provide managed card management and production services, where the Contractor owns, operates, and manages card management and production services and products at agency locations or Contractor locations, including the following:

(1) Ownership, operation, maintenance, and management of card management and production hardware and software.

(2) Provision of card management and production personnel.

The Contractor shall have the capability to provide managed PIV card management and production functions as specified in the following sections.

The Contractor shall have the capability to provide card management and production services and products that provide personalization of the physical (visual surface) and logical (contents of the ICC) aspects of the card at the time of issuance and maintenance thereafter. This includes not only printing photographs, names, and other information on the card, but also loading the relevant card applications, biometrics, and other data IAW FIPS 201.

The Contractor shall have the capability to provide the key management component for the generation of key pairs, the issuance and distribution of digital certificates containing the public key of the cardholder. The Contractor shall have the capability to provide the key management component throughout the life cycle of PIV Cards—from generation and loading of authentication keys and PKI credentials, to eventual renewal, re-issuance, or termination of the card IAW FIPS 201.

3.1.3.1 Card Management and Production Hardware and Software Compliance

Contractors providing managed card management and production services shall provide card management and production products only as part of managed services. The Contractor shall have the capability to provide card management and production hardware and software that comply with all requirements specified in Section 3.1.1 of this Qualifications Requirements Document.

3.1.3.2 Card Management and Production Deployment Services Compliance

The Contractor shall have the capability to provide card management and production deployment services as part of managed card management and production services that comply with all requirements specified in Section 3.1.2 of this Qualifications Requirements Document.

The Contractor shall have the capability to deliver quantities of PIV compliant PIV cards, with standard configuration and applicant personalization IAW FIPS 201 via secure shipping and delivery processes, including delivery tracking and confirmation, only to authorized locations and authorities.

3.1.3.3 Audit, Logging, and Standard Reporting

The Contractor shall ensure that the technologies and systems used to collect, validate, transmit, and store a PIV card applicant's information are in compliance with the PIV privacy policies, specifically in FIPS 201 for PIV cards, and allow for continuous auditing:

(1) The Contractor shall ensure that all identity and access activity shall have an auditable trail that can support forensic and system management capabilities, with the minimum capability to:

(a) Reconstruct the chain of trust for production and management.

(b) Reconstruct access events to a given logical and/or physical asset.

(c) Reconstruct access events by an individual card holder.

(2) The Contractor shall have the capability to provide a flexible sorting and reporting capability that allows information to be presented in graphical format, filtered and sorted as necessary to present usage, operations, security, auditing, and management information.

(3) The Contractor shall have the capability to provide the following four categories of reports:

(a) Audit Reports that shall provide data necessary to monitor, reconcile, and audit system processing and reconciliation.

(b) Program Management Reports that shall provide information that will be used to manage the organization's PIV services.

(c) System Performance Reports that shall monitor the operation and performance of the PIV card services system.

(d) System Fraud and Security Reports that shall provide information that will assist in the detection of fraud and ensure system security. At a minimum, data provided in System Fraud and Security Reports shall include the following information:

1 Attempts (by location) to log on to the system using invalid passwords.

2 Cards reported lost or stolen.

3 Disputed or erroneous transactions.

3.1.3.4 Technical Standards Compliance

All data output from the card management and production hardware and software products shall be in compliance with the following standards and guidelines, specifically in compliance with the data model and PIV object identifier requirements specified in FIPS 201 and NIST SP 800-76:

For those HSPD-12 PIV hardware and software products requiring compliance, the Contractor shall have the capability to provide a plan to ensure that all products are fully compliant with the following standards and guidelines and any certifications included in those standards:

(1) FIPS 201: Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Standards and Technology (NIST), March 2006.

(2) SP 800-73: Special Publication 800-73, Interfaces for Personal Identity Verification, National Institute of Standards and Technology (NIST), April 2005

(3) Employees and Contractors, Office of Management and Budget, M-05-24, DRAFT 5 August 2005.

(4) NIST SP 800-79: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, Publication No. 800-79, NIST, July 2005.

(5) NIST SP 800-76, PIV Biometric Data Specification.

(5) NIST SP 800-78, PIV Cryptographic Algorithms for and Key Sizes.

(6) NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

All card management and production products related to the PIV card for which compliance is required must comply with HSPD-12, Federal Information Processing Standard 201 (FIPS 201), applicable National Institute of Standards and Technology (NIST) Special Publications (SP) and/or GSA interoperability compliance requirements. For categories of card management and production products that require GSA approval (see http://fips201ep.cio.gov/index.php), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant products relate to provision of products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. NIST has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated

circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform tests for interoperability.

3.1.3.5 Interface and Interoperability Support

To support communications with authorized officials and users, the hardware and software shall, at a minimum, support World Wide Web (WWW) Internet network access and interfaces for telecommunications services. The products shall support other network access interfaces and/or protocols as agreed between the ordering activity and the Contractor.

The products shall have the capability to implement software and interfaces that provide digital signature, authentication, data integrity, and privacy of personal data at rest and during transmission.

The Contractor shall have the capability to provide interface and protocols for communications to support intra-operability among PIV components provided by the Contractor and for integrated solutions provided by the Contractor.

If the product and/or integrated solution interfaces to a PIV component (i.e., agency PACS, LACS, enrollment/registration system) provided by another Contractor or agency, the Contractor shall have the capability to implement the PIV interface specification specified by the Government.

The PIV interface specification to support interoperability between PIV components provided by other Contractors and/or ordering entities (i.e., agencies) is currently under development. The Contractor shall have the capability to implement and support the PIV interface specification, at the time the PIV interface specification is published and required for all Contractors under SIN 132-62.

3.1.3.6 Security Certification and Accreditation (C&A) and Re-Accreditation

The Contractor shall provide documentation of successful completion of a security audit related to card management and production services and products that was conducted by an independent, trusted third party. The security audit shall have been conducted on similar deployed government or non-government systems.

For managed services provided at agency locations, the Contractor shall have the capability to provide support for completion of C&A in accordance with Section B of FIPS 201.

3.1.3.6.1 Plan for Completion of Initial C&A

The Contractor shall have the capability to provide a plan for completion of security Certification and Accreditation (C&A) and for obtaining management Authority to Operate (ATO) from a Federal Government Designated Approving Authority (DAA) as follows:

(1) The Contractor shall complete security C&A as required for storing, transmitting, and/or processing government information in an information system and/or approved system components or products provided by the Contractor at the Contractor facilities, and

(2) The Contractor shall support security C&A as required for storing, transmitting, and/or processing government information in an information system and/or approved system components or products provided by the Contractor at Federal government facilities.

The plan for completion of C&A shall address the following:

(1) The Contractor shall complete C&A IAW with Office of Management and Budget Circular A-130, Appendix III; Federal Information Security Management Act (FISMA) 2002, NIST 800-79, GSA security policies, procedures, and guidelines, and the FIPS 201 that are in full force and effect as of March 1, 2006, or as subsequently revised. The documentation defining the applicable security standards and requirements for completing C&A shall be obtained from GSA.

(2) The Contractor shall have a security compliance audit conducted by an approved, independent trusted third-party and provide documentation of the results of the audit. That audit shall be conducted pursuant to guidance provided in the American Institute of Certified Public Accountants' (AICPA's) Statement on Auditing Standards (SAS) Number 70, Reports on the Process of Transactions by the Service Organizations, WebTrust Certification, and/or other applicable and approved guidance. The focus of this review shall be to provide the Government with independent verification that the Contractor is performing IAW with the applicable standards, requirements, FIPS 201, GSA policies and procedures, and this Statement of Qualification Requirements.

(3) The Contractor shall submit a C&A package in accordance with NIST SP 800-37. Guide for the Security Certification and Accreditation of Federal Information Systems, and the GSA security certification and accreditation guidelines and policies.

(4) The Contractor shall submit a Card Production Security Policy as specified in FIPS 201.

Documentation of applicable compliance audit requirements in force and effect at the time of security C&A shall be obtained from GSA.

3.1.3.6.2 Periodic Review of Security Controls

Periodic independent audits and reviews and re-accreditation shall occur IAW the standards and requirements in full force and effect on March 1, 2006, or as subsequently revised.

3.1.3.7 Date/Time Stamp Synchronization

The Contractor shall have the capability to implement date/time stamps as required for audit and logging of transactions and data. The Contractor shall use Coordinated Universal Time (UTC) NIST as the reference time base. Contractor's time shall be synchronized within one second and granularity of time expressed shall be at least to the granularity of one minute.

3.1.3.8 Performance

The Contractor shall meet, at a minimum, the performance standards as specified for the following:

(1) Hours of operation.

(2) Availability of services.

(3) Response time for services.

3.1.3.8.1 Hours of Operation

The Contractor shall operate the following on-line services 24 hours per day, 7 days per week, including Federal holidays:

(1) Application acceptance and renewal services.

(2) Verification and validation services.

(3) Immediate PIV card revocation services.

(4) Problem reporting.

(5) Change reporting.

All of the remaining services and products specified shall, at a minimum, be operated on the basis of a 5-day, 40-hour work week, Monday through Friday, except Federal holidays.

3.1.3.8.2 Availability of Services

All of the on-line services and products specified shall, at a minimum, be in operation and available for use during the required hours of operation, not less than 99.5 percent of the time calculated on a monthly basis.

3.1.3.8.3 Response Time for Services

The Contractor shall, at a minimum, have the capability to provide the specified services according to the response times set forth in Table 3.1.3.8.3-1. All response times shall be measured from the time the Contractor receives an initiation message in its inbound queue until

the time the Contractor's response leaves its outbound queue (i.e., from the time a request message is received until the time the response message is transmitted to the requestor).

Table 3.1.3.8.3-1. Response Time Requirements

Transaction/Process	Response	Constraints
On-site technical assistance	5 days	>= 95% of all transactions within response
Response to trouble call	30 minutes	>= 95% of all transactions within response
Replacement of hardware/software due to component failures	Next day shipping	>= 95% of all transactions within response

3.1.3.9 Customer Service Center

The Contractor shall have the capability to provide a customer service center to provide help desk and other support functionalities for card holders and ordering activities.

3.1.3.9.1 Services for Ordering Activity Applications

The customer service center shall assist authorized representatives of participating ordering activities as follows:

(1) Services, features, and options.

(2) Troubleshooting and problem reporting.

(3) Billing questions and issues.

(4) Implementation of services.

3.1.3.9.2 Hours of Operation

The customer service center shall be available 24 hours a day, 7 days per week.

3.1.3.9.3 Toll-free Telephone Service

The customer service center shall have the capability to provide toll-free telephone service.

Voice mail capabilities shall be provided for handling incoming calls received at times when assigned staff is unavailable.

3.1.3.9.4 On-line and E-Mail Services

The customer service center shall provide on-line information and support to all card holders (e.g., maintenance of a web site for posting Frequently Asked Questions (FAQs) and general information to help cardholders).

The customer service center shall provide an e-mail address for use by all card holders in communicating with the customer service center.

The customer service center shall respond to e-mail messages received automatically with a prompt acknowledgement of receipt and respond to content in a time consistent with industry practices.

3.1.3.9.5 Problem Identification and Resolution

The customer service center shall implement and maintain a system for receiving, recording, responding to, and reporting customer service problems within its own organization and to the Government.

3.1.3.9.6 Customer Service Records

The customer service center shall implement and maintain a system of records relating to customer requests for services and the services provided. For each such request, the Contractor shall record sufficient information in order for the Government to determine who requested assistance, when the request was submitted, what action was required and/or resolution of the issue, and when the issue was resolved. At a minimum, the Contractor shall record the following information for each customer service request:

(1) Date/time initially contacted.

(2) Method of contact (e.g., telephone, e-mail, etc.).

(3) Name of individual making the contact.

(4) Individual agency application (if applicable).

(5) Type of service requested or problem reported.

(6) Action taken.

(7) Date/time action completed.

(8) Name of person taking the action.

(9) Requirements for follow-up action (if any).

(10) Date/time report filed.

(11) Name of person filing report.

The Contractor shall provide the capability for customer service records to be made available for Government review or quality assurance inspection upon request.

3.1.3.10 Privacy Act Requirements

The Contractor will be maintaining one or more "systems of records" requiring protection under Section 552a, Title 5 of United States Code (5 U.S.C. 552a). The minimum standards for protecting and reporting on these systems of records are also set forth in 5 U.S.C. 552a. The regulations for protecting and reporting on these systems of records are set forth in Appendix I (Federal Agency Responsibilities for Maintaining Records About Individuals) to Office of Management and Budget (OMB) Circular Number A-130 (Management of Federal Information Resources).

Subsection (m) (1) of 5 U.S.C. 552a and Paragraph 3.a.(1) of Appendix I to OMB Circular Number A-130 provide that the systems of records protection and reporting requirements shall be passed through to any Contractor who maintains a system(s) of records on behalf of a Government agency.

The Contractor shall have the capability to meet the minimum systems of records protection and reporting requirements for the Contractor set forth in this Statement of Qualification Requirements.

3.1.3.11 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV services, HSPD-12, and FIPS 201. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.3.12 Data Transfer

The Contractor shall have the capability to initiate a complete transfer of all current and archived PIV card management data, policies and practices, billing, and audit data within 24 hours of request, or as otherwise agreed upon, IAW this Statement of Qualification Requirements, SIN 132-62, and according to Government-approved Data Transfer Plan. The Contractor shall maintain and keep up to date the Data Transfer Plan that is submitted as part of this Statement of Qualification Requirements. The data transferred shall not include any non-HSPD-12 services or non-government data.

3.1.3.13 Security/Privacy Requirements

3.1.3.13.1 Administrative and Personnel Security

The Contractor shall have the capability to ensure the integrity of managed service operations including all personnel involved in system administration, security administration, card management and production operators, on-site installation, troubleshooting, and training, and system configuration (i.e., operating system, software, and peripheral installations and configuration) services. The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing managed service operations.

The Contractor shall have the capability to enforce the principle of separation of duties to ensure that no single individual has the capability to issue a PIV card without the participation of another authorized person. The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

3.1.3.13.2 Privacy Requirements

Unless otherwise specified, the data on the PIV card shall be limited to Sensitive but Unclassified data. While not subject to the regulations protecting classified data, nevertheless, such data shall be subject to privacy protection IAW the Privacy Act of 1974.

3.1.3.13.3 Data Retention

The Contractor shall have the capability to retain and archive all HSPD-12 PIV data in accordance with Federal data retention laws and regulations as specified by the U.S. National Archives and Records Administration.

3.1.3.14 Past Performance

The Contractor shall have the capability to provide detailed descriptions of past performance and prior experience related to large-scale government and/or non-government similar implementations for the Contractor and any member of the Contractor's team (e.g., subcontractor, joint venture, etc.) responsible for providing an estimated 25% or more of the services and products provided under an awarded contract.

The Contractor shall have the capability to provide information related to past performance and prior experience for the Contractor's largest projects (considering dollar value) completed or ongoing with an end date for each selected project not more than two years prior to the release of this Statement of Qualification Requirements.

The Contractor shall have the capability to provide the following past performance and prior experience information related to the Contractor's selected projects:

(1) Compliance with technical or functional specifications or requirements.

(2) Technology refreshment.

(3) Quality of services and products;

(4) Adherence to schedules.

3.1.3.15 Deliverables

The Contractor shall have the capability to provide the following deliverables as listed in Table 3.1.3.15-1, Deliverables.

Table 3.1.3.15-1. Deliverables

No.	Descriptions of Deliverables	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
1.	Create and maintain such records as required for all data captured, stored, and maintained for each applicant.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.
2.	Create and maintain such records as required for each applicant's and card holder's identity information.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.
3.	A record of the transaction audit data resulting from deployment of the identity information to other system components and receipt of information from other system components.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.
4.	A record of the transaction audit data resulting from PIV card life cycle management, including issuance, re-issuance, replacement, renewal, revocation, and termination.	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request.

No.	Descriptions of Deliverables	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
5.	Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
6.	Program management reports providing information used to manage the PIV services.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
7.	System performance reports that monitor the operation and performance of the PIV services.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
8.	System fraud and security reports that will assist in the detection of fraud and ensure system security.	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
9.	Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or a plan for approval.	As required in qualification requirements response package.	As required n qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.

No.	Descriptions of Deliverables	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
10.	Security audit, or Certification and Accreditation (C&A) and Re-Accreditation documentation as specified in NIST Special Publications, or a plan for C&A.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
11.	Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media)	As required in requests.	As required in request.	As required in request.	Within 30 calendar days of receipt of request.
12.	A record of transaction audit data for each request received by the Customer Service Center	As required in requests.	As required in request.	As required in request.	Within 48 hours of receipt of request
13.	Provide assurance of the trustworthiness and competence of employees.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
14.	Data Transfer Plan	As required in request	As required in request	As required in request	Within 24 hours of receipt of request
15.	Fraud protection procedures	As required in request	As required in request	As required in request	60 calendar days from contract award

No.	Descriptions of Deliverables	Quantity	Medium of Delivery	Where to Deliver	Submittal Date
16.	Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse	As required in request	Electronically, mail, or facsimile	As required in request	Immediately
17.	Trouble reports status	As required in request for procedures	Electronically, mail, or facsimile	As required in request	Within 4 hours after first report, updated every 4 hours thereafter
18.	Technical meetings	As required in request	As required in request	As required in request	As required in request
19.	Monthly reports	One (1)	Electronic access, plus 1 paper copy	As required in request	Within 10 business days of the end of the month covered in the report.
20.	Data collection forms	As required in request	As required in request	As required in request	As required in request
21.	Request to establish a new or make a significant change to an existing systems of record reporting	As required in request	As required in request	As required in request	Not less than 60 working days prior to the requested implementation date.
22.	Information related to past performance as specified.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.	As required in qualification requirements response package.
23.	Implementation schedule and plan.	As required in request.	As required in request.	As required in request	As required in request.

3.1.3.16 Project Management Office

The Contractor shall have the capability to provide a Project Management Office (PMO) to oversee all facets of the managed card management and production services.

3.1.3.17 Managed Card Management and Production Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the card management and production managed services qualification requirements specified in this document as follows:

(1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified, specifically in the following "core" requirements.
   (a) All technical and functional requirements.
   (b) Past performance and experience in implementation of similar and/or equivalent enterprise services.
   (c) Documentary evidence (i.e., attestations) of a security assessment conducted by an independent, trusted third party, for a similar and/or equivalent enterprise implementation in accordance with Federal, international, or industry standard.

(2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services), the Contractor may provide a consolidated response.

(3) Documentary evidence of past performance as specified in Section 3.1.3.14 of this document.

(4) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA approval for those products that require FIPS 201 and GSA approval as specified in Section 3.1.3.4 of this document.

(5) Documentary evidence of competence of employees as specified in Section 3.1.3.11 of this document.

(6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.3.13.1 of this document.

(7) Documentary evidence of security audit, C&A, or plan for C&A, as specified in Section 3.1.3.6.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.2 Pricing

The Contractor shall have the capability to comply with the pricing requirements specified in SIN 132-62, this qualification and requirements document, and as follows:

(1) Pricing for card management and production workstations shall not include the costs for the physical space. Physical space at agency locations for card management and production workstations will be provided by the Government.

(2) All prices shall include all Contractor program management and administrative costs.

(3) Hardware pricing shall include hardware replacements during the first five (5) years.

(4) Software pricing shall include an annual maintenance price for updating with operating system patches and other software upgrades.

Appendix A: Qualification Requirements Submission Criteria

All information related to package submission in response to PIV Statements of Qualification Requirements is available at the GSA Identity Management web site: (www.idmanagement.gov), including statements of qualification requirements for all PIV services and products, application forms, submission instructions, and evaluation processes and procedures.

Contractors may submit requests for review of their qualifications in response to services and products in one or more of the following categories in this Statement of Qualification Requirements:

(1) Card management and production hardware and software products.

(2) Card deployment services.

(3) Managed card management and production services.

Contractors may also submit requests for review of their qualifications in response to one or more Statements of Qualification Requirements for other SIN 132-62 HSPD-12 services and products.

A.1 General Instructions

(1) The Contractor shall accurately complete the application cover sheet and submission package for the PIV services and products for which the Contractor is requesting review and approval.
(2) The Contractor shall provide evidence and deliverables necessary to enable the Government to determine compliance with applicable approval criteria.
(3) The Contractor shall provide technical staff, if needed, either onsite or via telephone, during the evaluation of the application and submission package.

A.2 Qualification Requirements Submission Contents

The contents of all submission packages in response to this Statement of Qualification Requirements shall be presented in three (3) sections as follows:

(1) Section 1- Technical: Section 1 shall include responses to all functional and technical requirements as specified for each category of services and/or products for which the Contractor is requesting evaluation.
(2) Section 2 – Past Performance: Section 2 shall include responses to all past performance requirements as specified for each category of services and/or products for which the Contractor is requesting evaluation.
(3) Section 3 – Security: Section 3 shall include responses to all security requirements as specified for each category of services and products for which the Contractor is requesting evaluation.

A.3 Consolidated Responses

To the extent the Contractor is submitting responses to multiple categories of services and/or products specified in this Statement of Qualification Requirements, the Contractor may provide a consolidated response.

To the extent the Contractor is submitting responses to multiple Statements of Qualification Requirements for PIV services and products, the Contractor may provide a consolidated response for the following:

(1) Section 2 – Past Performance. Section 2 shall include a consolidated response to all past performance requirements, including documentary evidenced, as specified for all PIV services and products included in the Contractor's submission package.
(2) Section 3 – Security: Section 3 shall include a consolidated response to all security requirements, including documentary evidence, as specified for all PIV services and products included in the Contractor's submission package.
(3) Documentary evidence related to the competence, integrity, and trustworthiness of employees.
(4) Documentary evidence of plan for technical standards compliance.

A.4 Compliance Matrix

The Contractor shall submit a completed Card Production and Management Services and Products Compliance Matrix as part of their response to the Statement of Qualification Requirements for PIV services and products.

Card Management and Production Services and Products

August 30, 2006

Compliance Matrix

Company Name

☐	Products
☐	Deployment Services
☐	Managed Services

Service/Product Name

Is this part of a consolidated response: Yes No

If Yes – indicate related services and products qualification requirements:

☐	Integration Services
☐	Activation and Finalization

☐	Enrollment and Registration
☐	Systems Infrastructure

TECHNICAL REQUIREMENTS:

Card management and Production Services – specific requirements – Section 3.1.1

NOTE: Provision of integration services requires integration of more than one HSPD-12 service and product.

Compliance Statement should be Concise: "We fully comply" or "We do not fully comply at this time." You need only fill out the areas applicable to what you are applying for. Some areas are required for all three categories of services: "Hardware and Software Products," "Deployment Services," and "Managed Services."

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
45.	Card Management and Production Hardware and Software Products - required for all 3 categories Supporting Proposal Section: :	3.1.1	
46.	Card Management and Production Software – required for all 3 categories Supporting Proposal Section: :	3.1.1.3	

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
47.	Hardware and Software Maintenance Support – required for all 3 categories Supporting Proposal Section: :	3.1.1.5	
48.	Deliverables Supporting Proposal Section: :	3.1.1.10	

Card management and Production Deployment Services – specific requirements – Section 3.1.2

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
49.	Card Management and Production Hardware and Software Products Compliance Supporting Proposal Section: :	3.1.2.1	
50.	Training - – required for deployment and managed services Supporting Proposal Section: :	3.1.2.2	
51.	Customer Service Center – required deployment and managed services Supporting Proposal Section: :	3.1.2.3 3.1.3.9	

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
52.	Availability of Services – required for deployment and managed services Supporting Proposal Section:	3.1.2.5	
53.	Response Time for Services Supporting Proposal Section: :	3.1.2.6	
54.	Scalability and Implementation Schedule – required for deployment and managed services Supporting Proposal Section: :	3.1.2.7	
55.	Project Management Office – required for deployment and managed services Supporting Proposal Section: :	3.1.2.13 3.1.3.16	
56.	Deliverables Supporting Proposal Section: :	3.1.2.12	

Managed PIV Integrated Services – specific requirements - Section 3.1.3

Req. No.	Description	Qualification Requirements Section References	Compliance Statement

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
57.	Card Management and Production Hardware and Software Compliance Supporting Proposal Section: :	3.1.3.1	
58.	Card Management and Production Deployment Services Compliance Supporting Proposal Section: :	3.1.3.2	
59.	Availability of Services – required for deployment and managed services Supporting Proposal Section:	3.1.2.5	
60.	Scalability and Implementation Schedule – required for deployment and managed services Supporting Proposal Section: :	3.1.2.7	
61.	Training - – required for deployment and managed services Supporting Proposal Section: :	3.1.2.2	
62.	Audit, Logging, and Standard Reporting Supporting Proposal Section: :	3.1.3.3	
63.	Date/Time Stamp Synchronization Supporting Proposal Section: :	3.1.3.7	

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
64.	Performance Supporting Proposal Section: :	3.1.3.8	
65.	Customer Service Center – required for deployment and managed services Supporting Proposal Section: :	3.1.2.3 3.1.3.9	
66.	Data Transfer Supporting Proposal Section: :	3.1.3.12	
67.	Project Management Office – required for deployment and managed services Supporting Proposal Section: :	3.1.3.16	
68.	Deliverables Supporting Proposal Section: :	3.1.3.15	

Qualification Requirements that are "Common" to all Integration Services and Products

Req. No.	Description	Qualification Requirements Section References	Compliance Statement

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
69.	Security Certification and Accreditation (C&A) and Re-Accreditation – see Security Requirements Evaluation Form		
70.	Privacy Act Requirements – See Security Requirements Evaluation Form		
71.	Past Performance – See Past Performance Requirements Evaluation Form		
72.	Technical Standards Compliance Supporting Proposal Section: :	3.1.1.1 3.1.3.4	
73.	Interface and Interoperability Support Supporting Proposal Section: :	3.1.1.2 3.1.3.5	
74.	Allowance for Technology Changes Supporting Proposal Section: :	3.1.1.7 3.1.2.8	
75.	Contractor Personnel Training Supporting Proposal Section: :	3.1.1.8 3.1.2.10 3.1.3.11	
76.	Special Contract Requirements Supporting Proposal Section: :	3.1.1.6 3.1.2.4	

SECURITY REQUIREMENTS:

Card management and Production Hardware and Software Products

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
77.	Security standards requirements Supporting Proposal Section: :	3.1.1.4	

Card management and Production Deployment Services

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
78.	Security standards requirements Supporting Proposal Section: :	3.1.1.4	

Managed Card management and Production Services

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
79.	Security standards requirements Supporting Proposal Section: :	3.1.1.4	

Req. No.	Description	Qualification Requirements Section References	Compliance Statement
80.	Security Certification and Accreditation (C&A) and Re-Accreditation • Documentation/attestation of previous security audit on a similar system. • Documentation of previous management Authority to Operate (ATO) on a similar system. • Plan for obtaining ATO	3.1.3.6	
81.	Privacy Act Requirements Supporting Proposal Section: :	3.1.3.10	
82.	Administrative Personnel Security Supporting Proposal Section: :	3.1.1.9 3.1.2.11	
83.	Security/Privacy Requirements • Administrative Personnel Security • Privacy Requirements • Data Retention Supporting Proposal Section: :	3.1.3.13	